Entendendo o que são malwares

Um dos problemas proeminentes que surgiu com a disseminação da tecnologia é o malware. Malware é um termo que abrange vírus, worms, cavalos de Tróia e bombas lógicas, bem como adware e spyware. Estes tipos de malware causaram uma série de problemas ao longo dos anos, que vão desde simples aborrecimentos a perigosos e maliciosos exploits. Softwares que se encaixam na categoria de malware, evoluíram drasticamente até incluir a capacidade de roubar senhas, informações pessoais e identidades, bem como danos hardware em alguns casos (como Stuxnet fez).

Malware é um termo novo, abrangente, mas os tipos de software que cobre estão longe de ser novos. Vírus e worms são algumas das mais antigas formas de softwares maliciosos existentes. O que mudou é o poder da tecnologia, a criatividade dos projetistas e o efeito de novos métodos de distribuição, como redes mais complexas, compartilhamento de arquivos peer-to-peer, conectados sempre à Internet e outros mecanismos que venho a tona durante os anos.

Veremos também os *covert channels*, cuja utilização aumentou gradualmente. Esses canais são componentes desconhecidos e não monitorados de um sistema que pode ser explorado para obter acesso ao sistema. Através do uso de um covert channel, um invasor poderá ser capaz de conseguir o acesso a um sistema sem o conhecimento do proprietário ou atrasar a detecção tanto que, no momento em que o ponto de entrada é descoberto, é tarde demais para o defensor fazer algo sobre isso.

Malware

Malware é um termo que é freqüentemente usado, mas frequentemente mal aplicado, então vamos primeiro esclarecer seu significado. O termo malware é abreviação de software mal-intencionado, que explica com precisão o que essa classe de

software é projetada para fazer: executar ações maliciosas e disruptivas.

Nas últimas décadas, o que chamamos agora de malware não era tão vicioso na natureza; Era mais benigna. Software nesta classe foi capaz de infectar, interromper, desativar e, em alguns casos, corromper outros softwares, incluindo o sistema operacional. No entanto, geralmente apenas irritando os proprietários do sistema; As formas mais desagradáveis ??eram raras.

Nos últimos anos, porém, esta categoria de software passou a incluir aplicações que são muito mais malignas. O malware atual é projetado para permanecer furtivo em muitos casos e emprega uma miríade de recursos projetados para impedir a detecção pelos sistemas de antimalware cada vez mais complexos e precisos, como software antivírus e antispyware. O que não mudou é o fato de que o malware consome recursos e energia em um sistema host ou rede, mantendo o proprietário no escuro quanto à sua existência e atividades.

Para piorar a situação no mundo de hoje, é que os tipos de malware atuais foram influenciados pelo elemento criminoso. A criação de botnets e roubo de informações estão se tornando muito comuns.

Malware é uma contração do termo “software malicioso”. Tenha isso em mente. O termo descreve com precisão a finalidade deste tipo de software.

Se definimos malware para incluir qualquer software que executa ações sem o conhecimento do usuário ou consentimento, isso pode incluir uma grande quantidade de software comuns. Também é importante reconhecer que a maioria dos malwares é de natureza hostil. Os criminosos usam malware de várias maneiras para capturar informações sobre a vítima ou cometer outros atos. A tecnologia tem evoluído, assim como o malware, do irritante para o completamente malicioso.

Outro aspecto do malware que surgiu é o seu uso para roubar informações. Programas maliciosos foram conhecidos para instalar o que é conhecido como um keylogger em um sistema. A intenção é capturar teclas, com a intenção de coletar informações como números de cartão de crédito, números de conta bancária e informações semelhantes. Por exemplo, o malware foi usado para roubar informações de pessoas em jogos on-line, para obter informações de conta dos jogadores.

Caso real no mundo

Um dos incidentes sobre os perigos de malware envolveu o varejista com sede nos EUA “Target”. No final de novembro até o início de dezembro de 2013, a Target se tornou a vítima de uma violação de dados que comprometeu pelo menos 110 milhões de contas de clientes: aproximadamente 40 milhões incluíam informações de crédito, débito e PIN e os 70 milhões restantes envolvem nome, endereço e informações de telefone. Este ataque, cujas consequências ainda estão sendo avaliadas, representa a segunda maior violação de dados da história.

O que permitiu essa violação? Os relatórios iniciais apontam fortemente para o fato de que o ataque foi possível, pelo menos em parte, por malware que encontrou seu caminho para os sistemas de ponto de venda usados ??no check-out.

As consequências deste ataque foram múltiplas. A imagem pública da Target foi manchada, seu preço de ação caiu e as vendas cairam enquanto os clientes questionaram se poderiam confiar na Target com sua informação. Além disso, a Target tinha de oferecer monitoramento de crédito para seus clientes, e muitos desses cartões de crédito e contas associadas dos mesmos clientes foram fechados e reeditados por seus bancos como uma medida de precaução. Finalmente, o Congresso dos EUA iniciou audiências no Senado para descobrir mais sobre a violação, com a assistência do Serviço Secreto dos EUA e da Federal Trade Commission.

Outro detalhes interessante para este incidente é o fluxo de informações que está disponível como resultado. O escopo do ataque e o fato de que ele era sem precedentes pegou o setor de varejo, como um todo, de surpresa. Isso resultou em um monte de informações sobre o ataque tornando-se público nas horas e dias seguintes à detecção e comunicação da violação. À medida que os dias prolongavam-se em semanas e meses e agora em anos, muitos dos relatórios iniciais desapareceram da web e as fontes ficaram tranquilas. Embora possa parecer duvidoso que essas informações desapareçam, a intenção foi benigna. Muita da informação detalhada que foi relatada foi removida de modo a não interferir com a investigação em curso e para evitar que um imitador em potencial realize outro ataque (ou pelo menos torná-lo mais difícil de fazer). A sabedoria deste movimento ainda está sendo debatida, mas destaca uma das questões de ser um hacker ético: Você deve ter cuidado com a informação e conscientes dos danos que podem ser causados ??se cair em mãos erradas.

Malware e a Lei

Os hackers éticos devem estar conscientes das leis que se relaciona com a implantação e uso de malware. Ao longo dos anos, o malware tem sido alvo de crescente atenção jurídica, pois a tecnologia evoluiu de ser inofensiva para muito mais maliciosa e expansiva em suas habilidades. A criação e o uso de malware levaram à promulgação de algumas leis muito rígidas. Muitos países aprovaram ou modificaram as leis para dissuadir o uso de malware. Nos Estados Unidos, as leis que foram promulgadas incluem o seguinte:

- **A Lei de Fraude e Abuso de Computadores** (The Computer Fraud and Abuse Act) – Esta lei foi originalmente aprovada para abordar ofensas federais relacionadas com computadores e o cracking de sistemas de computador. O ato aplica-se a casos que envolvem interesses federais, ou situações envolvendo computadores do governo federal

ou de instituições financeiras. Além disso, a lei abrange a criminalidade informática que atravessa linhas de Estado ou jurisdições;

- **A Lei Patriota** (The Patriot Act) – Este ato ampliou os poderes já incluídos na Computer Fraud and Abuse Act. A lei prevê penas de até 10 anos para uma primeira ofensa e 20 anos para uma segunda ofensa. Ele avalia danos a sistemas múltiplos ao longo de um ano para determinar se tais danos são mais de US $ 5.000 total. Vale ressaltar que a Lei Patriot expirou em 1º de junho de 2015. No entanto, em 2 de junho de 2015, várias disposições da Lei Patriota foram restauradas de forma modificada como parte da Lei de Liberdade dos EUA;
- **CAN-SPAM Act** – Esta lei foi concebida para impedir a propagação de spam: mensagens enviadas em massa que assediar ou irritar o destinatário na compra de produtos ou serviços. Cada país abordou o problema de malware de forma um pouco diferente, com penas que vão desde prisão até multas potencialmente íngremes para violadores. Nos Estados Unidos, estados como Califórnia, Virgínia Ocidental, e uma série de outros têm colocado em vigor leis destinadas a punir os autores de malware. Embora as leis tenham sanções diferentes destinadas a resolver os efeitos do malware, ainda tem de ser visto como essas leis são eficazes.

Sugestões de livros: